EU's Digital Future Seminar #2 - Assessing the Material Shaping of EU Digital Sovereignty in Response to the War in Ukraine

Brussels School of Governance - May 13 2024

Clément Perarnaud: Welcome everyone. I think we can get started. Welcome to this second seminar of our new seminar series on the EU's digital future. After a successful and intense first seminar in which we reflected on the trajectory of the EU in regulating the digital, it is my pleasure to welcome Professor Niels ten Oever from the University of Amsterdam for this new public event.

As some of you may remember from our first seminar, we had already touched upon important shifts that have characterized the EU approach to digital policies in recent decades, in recent years, and which could also prove instrumental in understanding the future decades. One of them being the rise of the discourse around EU digital sovereignty, which will be front and center in today's meeting.

While we had focused extensively about the internal politics and policies of the EU, today we're going to be a bit more outward looking and explore one of the international instruments through which the EU may have started to shape its digital sovereignty, namely international sanctions.

While sanctions have long imposed, have long been imposed on the exports of digital technologies, the EU in the context of the Ukraine war seems to have introduced a number of measures that seem very relevant for understanding of EU's digital sovereignty and its approach to the Internet. To impact those developments, we are

extremely lucky to have Niels ten Oever with us. Niels is a leading scholar with a rather unique voice in this academic space. He's also an assistant professor at the University of Amsterdam and co-principal investigator with a critical infrastructure. His recent research is focusing on how norms, values, and ideology gets inscribed, resisted, and subverted in communication infrastructures through their covenants, which is exactly the an analytical lens that you will be applying today in the study of recent EU sanctions.

This presentation will be discussed by Professor Roxana Radu, Assistant Professor at the University of Oxford, to whom I'm extremely grateful for accepting to be with us today and discussing this new research.

Thank you very much once again for joining us this afternoon, and I will now pass the floor to Niels. Thank you very much,

Niels ten Oever: thank you so much, Clément. Thanks so much, everyone. I am really thankful to Clément and the Brussels School of Governance for inviting me, and very much for Professor Radu for acting as a discussant and looking forward to the discussion.

Thank you all for being here on this, a rather sunny afternoon in Amsterdam. I'm Niels ten Oever and I'm with the Critical Infrastructure Lab. At the Critical Infrastructure Lab, we research how through the lenses of geopolitics, standards, and environment, how infrastructures are shaping today's society. We do so to seek to understand if we can develop future infrastructural futures that center people and planets over profit and capital. A project of the Critical Infrastructure Lab is trying to undo some of the work that the neoliberal university is doing because we firmly believe that knowledge creation is a social and a group process and not of an individual professor.

This is also reflected in the paper that I'll be discussing today, namely the paper that is currently under review, Sanctions and Infrastructural Ideologies, Assessing the Material Shaping of EU Digital Sovereignty in Response to the War in Ukraine. Just to make sure that you'll get the abstract or the too long didn't read version, that is that the EU sanctions against Russian entities are inconsistently implemented across the European Union member states. For the European Commission, this might be a breakthrough for its digital sovereignty agenda, because the Council and the Commission were aligned in establishing a digital sovereignty policy that combines economic sanctions and battling of misinformation.

Multistakeholder Internet governance functions as an ideological state apparatus guided by an infrastructural ideology to increase global connectivity on the interconnection layer, while the EU functions as an emerging repressive state apparatus by inscribing its norms through its territorial power in a part of the global network of networks, but only does so within its borders and on the content layer, and does not seek to do this outside of its borders.

This gives rise to a global ideological state apparatus which increases interconnection, while repressive state apparatuses inscribe their regional norms in a process of meta-governance of Internet governance. With the debate of cyberspace sovereignty by different authors, this meta-governance process might actually be what we are seeing, is what we theorize.

So, now you already know what we're going to do, so you can sit back and relax and have a bit of a look at this paper, which is real interdisciplinarity at work, because you see here, the co authors of this work are Clément Perarnaud, but also John Kristoff, Moritz Müller, Max Resing, Arturo Filasto, and Chris Kanich.

Even though in computer science it's very common to have a lot of authors, in our field it's not that common to have these many authors. I'd argue that it was really needed to do this work, because if we want to study the Internet and not just study what is said about it, its sociotechnical imaginaries or the discursive claims that are made about the Internet, but also how it really works, it's so crucial to have people from different backgrounds, expertises and experiences with us. This really also led to fascinating discussions and a quite elaborate method that I'll present in a little bit.

Our main research question is how do sanctions aimed at Internet infrastructure align with the EU's approach to Internet governance and digital sovereignty aspirations? In our methodology, we used a threefold approach.

First, we engaged in network measurements where we used venture points from different networks, namely from RIPE Atlas, EduVPN, DataPlane dot org, NLNOG RING, and OONI. This provided us with vantage points from from different member states in the European Union, but also from different networks within these member states, so that we could really make claims about how sanctions are being implemented.

We did that by measuring for reachability through DNS responses, by checking TLS handshakes and HTTP connections. We did so against a list of different entities, namely Russia Today, RT in Spanish, Sputnik, and a lot of lists that you can see that we got from different sources in different annexes to different decisions, namely council decisions, but also information provided by a national regulatory bodies.

And then, the third part of this was doing the classic Yanow conducting interpretive policy analysis of public documents from the EU and member states published from 2019 to 2024, which really corresponds to the underlying presidency, and we tried to look for EU digital sovereignty policy documents, and policies and processes that have accompanied the sanction development and implementation.

As you know, sanctions are known to be economic, diplomatic, militarily, sports, and environment. We have here a timeline that you see on the right side, which I got from an excellent report produced by Farzaneh Badieh, which was published on the RIPE website, which shows that sanctions on the Internet in Europe go back to 1999,

sanctions against Serbia, against satellite connection provided through to Serbia during the Yugoslav war. So, while you might be thinking that the current war in Ukraine, Starlink and satellite is providing new questions to Internet governance, actually many of these questions that we have here are very old because sanctions are a classical tool in the states' toolbox.

Economic sanctions are commercial and financial penalties applied against states, groups, or individuals, so these can be trade barriers, asset freezes, travel bans, arms embargoes. or restrictions on financial interactions. There is a lot of debate about sanctions, where the people argue that they are effective or ineffective.

Many people argue that it's not elites that are making the decisions that are being targeted, but rather the people, which led to an evolution in sanction studies and the implementation of sanctions guided to more targeted sanctions, but there is also the problem that often it's not the state that is handing out the sanction, is not the one implementing the sanctions, and this leads to heterogeneous implementation, or even to over-compliance where implementers try to stay two steps away from the county line and implement more than is asked for, and thus undermining the effectiveness of sanctions.

We're trying to combine these three concepts, namely sanctions, digital sovereignty, and network filtering, and see whether this amounts to an EU digital sovereignty process.

Sanctions in the European Union are proposed by the High Representative of the Union for Foreign Affairs and Security Policy. The High Representative introduces these sanctions to the Council, and it introduces it to the Council because it's part of the security policy and that's why it's done in the Council and not by the Commission.

The European Council, of course, consists of government ministers from each EU member state, and, when sanctions are adopted, it is the responsibility of the individual member states to implement these sanctions, but the European Commission oversees and evaluates the uniform application of the sanctions.

If we look at European digital sovereignty, there is a lot of debate, there is a lot of policy that have come up, but, thus far, as the scholar Clément Perarnaud says, European digital sovereign policy impacts are uncertain at best. This really is Clément playing on an understatement, because there is a lot of talk about it, but it's very hard to see what the EU tries to do, because it's trying to be open at the same time, it also tries to stimulate its own industry at the same time, but it's finding very hard because it wants to keep an open market.

So, then, the war in Ukraine, a quick timeline. In February 2014, Russia invaded Ukraine with an annexation of Crimea, an illegal military operation in Ukraine's eastern Donbas region, and then the EU created two sanction packages.

After February 2022, when Russia started a full scale invasion attempt of Ukraine, these sanctioned packages have been updated with continuous new information until Council Decision 2022/351 which read that it shall be prohibited for operators to broadcast or to enable, facilitate, or otherwise contribute to broadcast, any content by the legal persons, entities, or bodies listed in the Annex 15, included through transmission or distribution by any means, such as cable, satellite, IPTV, Internet service providers, Internet video sharing platforms or applications, whether new or pre-installed.

This was really an innovation to see how broadcast language is now being applied to the Internet and communication infrastructure.

What we then see in the literature, for instance, Caser-Ripolies et al saying they qualified this term as unprecedented and controversial, and part of strengthening the EU's geopolitical approach towards disinformation. Helberger and Schulz argued that, before the start of the war, such a decision would have been considered unthinkable at EU level, in light of its scope, covering both audiovisual and online media, and its consequences for freedom of expression and access to information, Article 19 to the Universal Declaration of Human Rights, but also because media regulation as a cultural competency has been mainly left to the responsibility of EU Member States until this point in time.

So, in normal circumstances, Cabrera Blázquez argues, the EU does not have the competence to impose on Member States restrictions on the activities of a broadcaster under media law.

Here we see, as Portela tells us, that sanctions have become the tool enabling the Commission to give more substance to its geopolitical agenda. We argue that, with this list, the EU might have found a way to give an operationalization of its digital sovereignty agenda.

But, when we then look at the actual measurements -- on the left you see the different domains, and in the bottom you see the different countries -- we see a very heterogeneous implementation of the blocking access to Russian sanctioned sites.

Here you see again a lot of the different member states on the top, the number of autonomous systems that we have measured in each country, so these are many, the upstream DNS resolvers and the networks, and then for all the domains we have checked, and you see that where there is a zero or purple, it's completely blocked, and where it's 100, it is completely accessible.

So, you see that actually, even though rt dot com is the best blocked site, or the most effectively block site, there is still a lot of variety in not only in the scope, but also across the countries and across the different websites, and if you then see it on the different methods in which it has been implemented, we see there is also a wildly varying in the methods that is being used to block.

And then, when it is blocked, users are informed in very different ways. Sometimes users get an HTTP error code 404, which is service is not available, but actually, there is an HTTP status code that should mark unavailable for legal reasons, which is HTTP error code 451, but we haven't seen any implementation of this error code correctly.

There are also a lot of blocked pages in case, and then some pages say it's blocked based on existing legislation, but does not refer to the existing legislation, nor allow for due process and to read the actual determination, in some cases there is a concrete link, in some cases it is provided in different languages. But, in some cases, it has been actually just said, this is a short technical maintenance and it will be back shortly.

So, here we also see that users are not really informed about the reasons and the scope and possibility for due process.

Then, what we also saw is that the digital minister of Ukraine, Andrii Nabok, approached ICANN and RIPE to ask for Russian IP addresses and SSL certificates to not be handed out anymore, and the executive board of RIPE NCC and also ICANN responded immediately, and the executive board of RIPE NCC said it believes that the means to communicate should not be affected by domestic political disputes, international conflicts, or war, and this includes the provision of correctly registered Internet numbering resources.

But, the argument of Andrii Nabok was that Russians were directly attacking not only sovereign soil, but also communication infrastructure of Ukrainians, and this has also been effectively shown by Kevin Limonier and Louis Pétiniaud, how we see a topological representation of the conflict on network topology level.

But here, the executive board of RIPE NCC said it's committed to taking all lawful steps available to ensure that the RIPE NCC can provide undisrupted services to all members across its service region and the global Internet community, and the RIPE NCC executive board did so in response without consulting its members through the normal policy development processes, but issued this response immediately, and so did the ICANN President.

What is interesting is that RIPE NCC says here that it will do everything it can to service all its members, and one of the members here from the RIPE database is the Federal Guard Service of the Russian Federation, also, several weapons factories have an autonomous system number registered with RIPE.

So, here you see different levels where the EU is talking about the regular broadcast of content, but when it comes here to a concrete request to infrastructure providers, we see a direct a no from the organizations that run these resources, and what we then subsequently saw is that the RIPE NCC was also outside of the sanction package, so it was still possible for RIPE NCC to serve its members, and that having customers from Russia for RIPE was not part of the sanctions.

So, as first of three conclusions, namely considering the sanctions, the sanctions against the Russian entities are inconsistently implemented across the EU, and this can at least be attributed in part to the high level and technology-neutral description of the sanctions and the lack of recommendation for technical implementation, even though, for instance, the Bundesnetzagentur, the German regulator, provided guidance, and this guidance was actually quite widely followed across the EU, to the extent that there wasn't a homogeneous implementation.

Implementation of the sanctions was largely left to the interpretation of network operators, and guidance and interpretation provided by national authorities in EU member states, but only a few did so.

The technical methods used for implementing the blocks were not transparent in most cases, and end users are not adequately informed, or the reason they cannot access the requested resource, and that it's due to EU mandate filtering.

It is still very easy to find content from Russia Today and Sputnik Online, both through mirror sites as well as aggregate sites.

So, while these sanctions can be categorized as an economic measure, these sanctions might also be understood in the broader context of recent EU policies tackling online disinformation and foreign interference. The diffuse implementation might be basis to say that it had limited impact to increasing EU's digital sovereignty, however, this is a first large online content regulation measure by the EU, so, in terms of law and practice, it's a very huge step, even though the implementation thus far is not very advanced, but the evaluation of these policies by the Commission might lead to more uniform implementation.

To theorize what happened here, we argue that the multistakeholder Internet governance regime functions as an ideological state apparatus guided by an infrastructural ideology to increase interconnection, and we see this reflected in the response by ICANN and RIPE, that what they do is increase interconnection and facilitate everyone to connect to the Internet.

We also see that the repressive state apparatus, namely governments, as Althusser describes them, are providing leeway for the ideological state apparatus to produce this infrastructure based on interconnection, but the EU, in its turn, functions as an emerging repressive state apparatus by inscribing its norms through its territorial power as a part of the global network of networks, but only does so within its border and on the content layer. It doesn't seek to project its power beyond its borders or on the global network, it doesn't seek to limit the broadcasting or the provision of services of Sputnik of Russia today to the rest of the world, but only limited to the European Union.

So, a global ideological state apparatus to increase interconnection exists, while repressive state apparatus inscribe their regional norms in a process that we call the US of Internet governance. While we see repressive state apparatuses in the US, in Russia, in China, in Europe, and in many many other nation states, there is still an infrastructure of interconnection, and there is a repressive state apparatus trying to inscribe its its own norms. By calling this meta-governance of Internet governance, we show that this is actually one system, but that the one is optimized through an infrastructural infrastructural ideology of interconnection, and the other is through an infrastructural ideology of regional and local norms, and then, together through a dialectical process, they provide the global communication networks that we have today.

Here are some of the references of the work, and I'm greatly looking forward to the discussion and to make this paper more relevant and more understandable if need be.

So, I'm greatly looking forward to your comments. I'm very sorry I went a bit over time.

Clément Perarnaud: Thank you so much, Niels. No, no, you didn't, you really stick to the 20 minutes limit, and thank you so much for your presentation. I might be a bit biased, but I find it really fascinating.

And we are now going to hear from Roxana to discuss your research.

Thank you so much, and please, Roxana.

Roxana Radu: Hello, everyone, and thank you very much for the opportunity to join you and to listen to this fascinating research. It's a timely contribution, and I really appreciated the more critical approach you took, as well as the interdisciplinary methods you were using.

I think we're rarely really seeing that interdisciplinarity coming together in a paper in such a neat way. It's usually a bit forced and it's hard to make sense of that in the Internet governance context, but here, the way you applied it was quite straightforward.

I have a couple of comments, and I'll keep this short, just to say that the discussion around sanctions brought me back to some of my own discussions with my PhD supervisor back in the day. He is one of the leading experts on sanctions, and we went through all the targeted / non-targeted discussions and so on, and covered that in quite a bit of detail, only to realize that communications have always been that. gray area. It has never really been, let's say, clearly mentioned within these different sanctions regimes, although, of course, we have the case of Serbia where there's an invocation of the charter of the UN, but beyond that there isn't much, so I appreciate the novelty of combining these different streams of research.

On what you have presented, I think my main comment has to do with how you situate this in the broader EU context, and the discourse on digital sovereignty, because I felt the link there was not very clearly articulated.

On the one hand, we have the EU Council decision, but of course this is not the first time the EU has actually imposed sanctions against the malicious actors, if you want, that's the terminology that the EU has been using in the EU Cyber Diplomacy Toolbox. There are a couple of decisions within the common foreign and security policy of the EU that are specifically labeled as cybercrime, so it would be good to know how this particular Council decision from 2022 differs from the existing set of sanctions that the EU has applied in the past, or that the EU is working on as part of its Cyber Diplomacy Toolbox.

You showed us very clearly that there is this heterogeneous implementation of this Council decision, and there I was very much looking for a causal link, and if at all it's possible to establish this kind of link based on your research, I would really encourage you to push it a little bit further, because there are two different pathways that need to be cleared in that discussion. One is to express in a more concise and direct manner who is actually responsible for implementation at the national level, and whether there is capacity or monitoring that would be based on some sort of assessment to do that in a consistent way.

But then, secondly, it would be really important to distinguish more clearly between institutional mandates from what RIPE NCC is doing all the way to what some of the national authorities might be mandated to do, in particular, when it comes to disinformation, as this seems to be the main targeting of this Council decision.

Admittedly, there is no other work doing that before, so I think you are really a pathbreaker here, but it would be really good not to combine all these different things in one conclusion, but actually tell us where that conclusion comes from. Maybe this is already in the paper, but I think in the presentation, it didn't come through as much.

Finally, on the theoretical anchoring, I would have appreciated a strengthening of the connections with the digital sovereignty discourse. I felt it remained a little bit disconnected from it. You have there lots of different declinations of that particular discourse, one is technological autonomy, the other one might be strategic autonomy, then we could argue there is now the emergence of this particular stance towards disinformation operations. I think you would need to advance that kind of work on digital sovereignty to understand better how this is fitting within the meta-governance of Internet governance.

This would be my suggestion to take this forward, if you can, but I really appreciated the hard work that went into the paper, and the fact that it became an eye opener for the current policy discussions we have. Thank you very much.

Clément Perarnaud: Thank you very much, Roxana, for this discussion and those comments.

Maybe Niels, if you want to already react to those comments, and then I will have a few questions for you as well.

Niels ten Oever: Thanks so much for those super thoughtful comments, Roxana.

There is still a lot to be done, and I think we tried to come up with a method and measurements and theory and combining legal with the measurements and a theory that would explain it all, but I think this is also really a pain that we felt of interdisciplinary or transdisciplinary work, even. There's, of course, this classic understanding, there are no borders in the Internet. So, where do you measure? Where are the networks? On which level do you measure in the networks? From where do you measure? From where do you have a comprehensive view? What happens in a country? What is a digital country? So, that was interesting for us.

And then, by looking at it, that is also a huge problem for the national regulators, and the national regulators have already been are already faced with a wave of work after the GDPR, and now they see the DSA, the DMA, and everything coming at them. When we talk about sanctions, they were like.... they're like, yeah, this is not a priority for us at the moment, whatsoever.

I think that this might just be the Commission and the Council dipping their toe in this work, because a lot of the digital sovereignty work has had a lot of visibility, but not so much material translation, and then maybe what we see here is actually innovative material governance, or see like maybe this works? Because, on the other levels there was always a lot of tug on what digital sovereignty could be, and then a lot of discursive action, but not so much material action.

So, this is what we're trying to explore, could this actually be in a completely different place where we expected it to work, be the operationalization of digital sovereignty, and that maybe also explains why it's not so strongly anchored with the literature, but we should do better work to explain that, and I'll work on that.

I wanted to mention also RIPE and ICANN, because it was so clear that there was a direct request to them, but they chose not to respond, they explicitly chose not to implement the request, it was then addressed on another level of the stack. So, I think here we see the interconnection layer and the content layer happening in different realities, and that reality is not just a technical reality, but starting to also be a policy reality.

Maybe we see here a bit -- but now we're really connecting everything to everything -- the public core of the Internet, that we really see this lower layer of interconnection, that we see an emerging consensus, that we're not going to touch that.

What Keller Easterling says is that infrastructure is setting the invisible rules of everyday life, and the rules to a globalizing world are written in the language of infrastructure, and not in the language of law and diplomacy, because many law and diplomatic processes are at such a standstill at the moment.

I think the world sees that, and whereas, in the era of the telegraph, where a lot of sanctions were implemented as well, the first thing that would happen with a conflict would be the cutting of cables, right now we still see an increase of interconnection, globally, actually. So, I think there seems to be an emerging global consensus of not splintering on the interconnection level, and I think that's something that's really worth highlighting.

Where we tend to talk a lot about fragmentation and splintering, I think it really helps to also show that it hasn't splintered, and that's the really big thing, because, historically, that's what would have been expected in such times of geopolitical tension, and that, we've been trying to contribute to theorizing a bit.

So, I did not do right to all your comments, but I'll really try to do that in the revision of the paper, and, really, thanks so much for your very thankful remarks.

Clément Perarnaud: Thank you so much, Niels, for also bringing the part of the article which actually addresses the topic of Internet fragmentation, and put those renewed debates around this notion, and what this sanction means for this issue of fragmentation.

I've seen a hand raised from Romain Bosc, so I will try to allow you to speak, thank you.

Romain Bosc: I am Romain Bosc, I'm actually working at the RIPE NCC . I'm a public policy officer at the RIPE NCC, and I find the topic and the paper's angle very interesting.

First of all, I believe it is an under-researched area, especially the one on sanctions, which is very active in Europe these days, so I really appreciate this effort to put more research into that, and, of course, this is a priority for the RIPE NCC now.

From what I heard, I really find interesting that you take the position of the RIPE Executive Board, basically claiming that the Internet, the global Internet infrastructure should not be subject to political disputes and conflict, which, if you believe in the primary function of the RIPE NCC, which is basically to allocate and administer IP addresses and Internet numbering resources, makes sense.

Indeed, in a more geopoliticized world, making this claim sounds indeed, maybe, some kind of ideological statement, but it would be interesting to dig a bit deeper into the technical neutrality arguments, as opposed to the the more foreign policy tool of which a sanction is part.

One concrete example is, what are the technical impacts of having Internet resources numbers sanctioned, so frozen, does it create a risk for the integrity and stability of the network? And not just seeing this as the effects of banning specific media, because here we are indeed at the upper layer of of the Internet technology stack, which is the content layer.

Does it really risk the global Internet to have Internet numbering resources frozen, because one of the effects of this means that creates discrepancies between the registry function of what the RIR, like the RIPE NCC, is actually fulfilling, and what happens on the ground in terms of routing policies and routing decisions?

This is one aspect that we are actually shedding the light upon, and this is also an area where more research is required. So, the technical implications of the sanctions in terms of integrity and stability and security of the networks, that would be my suggestion.

I don't know if I'm being clear, but I'm happy to explore.

Niels ten Oever: No, no, it's extremely valuable, and I thank you very much for for posing this and for bringing this up.

As a science and technology scholar, every time I hear neutrality, I get a bit of, like, Ooh, but whose neutrality? Neutrality of what? Neutrality for whom? Right? What gets inscribed, and who decides what is neutral and what are the governance processes for that?

Romain Bosc: No, exactly. This is exactly what might require a bit more academic analysis, because, again, in a geopolitical world where everyone is actually opposing the principle of neutrality, it becomes interesting to see what are the implications in terms of political choices? Do we really want to keep the Internet interoperable and global if it becomes a vector for cyber attacks, in this interconnected and interdependent framework, which is the Internet? Do we want to keep it as one?

That's a primary question, especially if we doubt that some players are just working to make it still a one and interoperable network of networks. What is the cost of this? Do we want governments to actually shut that down, so we all evolve in respective bubbles, where it becomes a bit harder to actually, from a cyber attack perspective, other networks or other parts of the Internet, because in the end we are living in a splinternet,

so what is the cost of the splinternet and what is the cost of the one global interoperable network?

Because, if we doubt that some actors are just working for the technical implications of the network itself, without having an agenda that is supported by vested interest, then we put the entire Internet at risk.

I believe so.

Clément Perarnaud: Maybe if you want to answer this question Niels, and also one or two others, because I you been contributing also to the sanctions dot net project, and in this paper you also cover a bit what does this heterogeneous implementation of sanctions means for the application of sanction and sanction practices, so I wonder if you want to elaborate a bit on these aspects.

And, the first question of Roxana was about interdisciplinarity and I was wondering whether you would have suggestions for scholars for how to engage in such interdisciplinary work, and how to connect with computer scientists, so maybe explain a bit the approach, because I'm sure it's going to be really useful for others in the group. Thank you.

Niels ten Oever: Please allow me to first respond to Romain.

What I think is really quite interesting, what we try to theorize, and I think this could perhaps in part contribute to what you're looking for, is that countries do not necessarily seem to want to disconnect, because if China wanted to disconnect, it could have started its own numbering system, and so a lot of countries still want to live in this global connected world with a unique numbering system, but, at the same time, they want to inscribe their own rules, and sometimes this is presented as a zero sum game.

What we see is actually things are happening at the same time, and this is what we're trying to theorize, that what industry is really good at is increasing interconnection. It's what it does really well, and states are just not that good at it. What states are really good at is coming up with the rules and regulations and defending individual rights.

So, this is how I think, how there are different instruments that are trying to fit on top of each other now, and this is why we try to come up with these two different regimes, that do not necessarily work against each other, but simply have different functions, and that's why we come up with this notion of ideological and repressive state apparatuses.

That is way more elaborated in the paper. I'll not set up a whole seminar on Althusser here. I really appreciate the comment, Romain, and this also gives me a bridge to talk to interdisciplinarity, because working with people such as from RIPE has been a really

great jump to work interdisciplinarily, and also using tools such as the RIPE Atlas to do measurements.

As a humanity scholar, I was trained as a philosopher, trying to run your own network, and try to understand what's going on, provides such a profound and rewarding engagement with the material infrastructure, so I've done that with the Internet. We're also doing that with 5G, and then connecting to your own network, really helps you understand what's actually going on.

So, I gave a lot of talks before I was an academic, I was in civil society, and the first thing that civil society organizations would say, like, Sorry, but we're not technical. We really cannot say that anymore. In a time where the last thing you see before you go to bed, and the first thing you see when you wake up is this.

Niels ten Oever: But, even Aristotle argued that techne, that technology is what makes us human. This is when we wrote like How the Internet Really Works. Trying to understand is also like being able to critically relate to your environment, so it's also playing, engaging, and also a lot of the engineers really like to talk about their work, so it's also an invitation to go to other conferences, to work with other people, and to engage in other publication processes, and then work out these problems.

Actually, yeah, it's fun, and I find it also very rewarding because, in the end, we need to come up with solutions ourselves, because also states, the diplomats, also don't have the technical or the theory background to make this up, so this is again a call for interdisciplinary work, and for which multistakeholder platforms work really well to engage and have the privilege to work with all these different actors and catch that information.

Here I have to say again that the Internet is much better than the telecommunications sector at having information publicly available about how things work, about how things are registered, and about how to do measurements, and that's what allowed us to come to the conclusions that we have here, because doing such research on telecommunication networks is really much harder, and that might be a problem in the future where we see centralization of the Internet, and also merging of telecoms and the Internet, and so that might prove to problematic or an obstacle for future measurements on the Internet.

Clément Perarnaud: Thank you very much, Niels. I propose that we move to the end of the seminar, this allows me to to thank everyone for their participation. I just wanted to take this opportunity to flag that we will have be having a third seminar on the 20 of June, we will be hosting Professor Nathalie Smuha to talk once again, take this critical stance around EU digital policies, and reflect about the future of AI regulation after the AI Act. She's a legal scholar, but also a philosopher at KU Leuven, and she will add a lot about what to expect in the coming future.

Niels, I'll give you the floor, but just to thank you once again for your participation, and I look forward to seeing you again for the next seminar. Thank you.

Niels ten Oever: Thank you so much, Clément. Thank you everyone for being here. If you like this kind of work, the Critical Infrastructure Lab has two open reading groups, they meet biweekly, so every other week you can meet with a group to read about infrastructure, technology, and environment. The PDFs are there on the website. Feel free to join on Zoom, and else I'm great looking forward to see, cite you, and talk with you all, and if you have any question or comment, feel free to drop me an email as well.

Bye all.

Clément Perarnaud: Thank you everyone. Bye, everyone.